Privacy and Security Policies for the Web:

Government Access to Communications and Stored Data

James X. Dempsey

Center for Democracy & Technology

http://www.cdt.org

Santa Monica and San Francisco

December 2008

Basic Principles

Whatever information exists about you (the consumer), the government can get

Whatever information you (the service provider) store, the government can compel you to disclose (subject to generous relevancy and burdensomeness standards)

The best privacy policy usually yields to a subpoena, the worst allows disclosure upon “request”

The only question: what is the standard for government access/compulsory disclosure?

What Is the Standard for Government Access?

1791 - Fourth Amendment

1968 – Wiretap Act, aka Title III, 18 USC 2510 et seq.

1978 – FISA, 50 USC 1801 et seq.

1984 – Cable Act – 47 USC 551

1986 – Electronic Comm Privacy Act – 18 USC 2701 et seq

1994 – CALEA (location info) – 47 USC 1002(a)(2(A)

1996 – Telecom Act – 47 USC 222

2001 - PATRIOT Act – National Security Letters

2008 – FISA Amendments Act

Four Dominant Dichotomies

1. Stored in the home or on the person
vs. stored with a third party

2. In transit on the network
vs. stored on the network

3. Communications content vs. transactional data

4. Private spaces vs. public spaces

Six disruptive trends

1. Cloud computing
2. Search
3. Location awareness
4. Identification
5. Sensing
6. Interoperability

One Email - Eight Standards

1. Draft email stored on desktop - full 4th A protection.
2. Draft email stored on gMail – Stored Communications Act (SCA) – 18 USC 2703(b) – subpoena.
3. Content of email in transit - *Katz* - 4th A but no notice – federal Wiretap Act - court order based on probable cause (with special protections).
4. Content of email in storage with service provider 180 days or less – SCA 2703(a) – court order, probable cause (w/o special protections).
5. Content of opened email in storage with service provider 180 days or less – in dispute - see Theofel (9th Cir 2004).
6. Content of email in storage with service provider > 180 days - SCA – 2703(b) subpoena - no judicial approval. Contra, on 4th A grounds, Warshak (6th Cir 2007, rev'd en banc).
7. Transactional data about email - in transit - court order, pen/trap standard, 18 USC 3123 - very weak. Accord, Forrester (9th Cir 2007).
8. Transactional data about email - in storage - court order, 18 USC 2703(d) - intermediate standard.

Inconsistent Standards

- Book reading
  - Borrowing a book at the library – state library privacy law
  - Reading the same book on Google Books - ?
  - Adding the same book to your Google Books library - SCA
- Medical records
  - Stored in the doctor's office – HIPAA
  - Same records stored in a PHR with Microsoft – SCA or nothing

Inconsistent Standards - 2

- Watching a movie in your home
  - Watching a movie on a cable channel – Cable Act privacy provision
  - Renting the same movie on DVD from Netflix – Video Privacy Protection Act
  - Watching the same movie streaming from Netflix – maybe VPPA
  - Watching the same movie on YouTube - ?

Practice Tips

Compliance

If the request seems unreasonable, push back

Counseling

Collect less, retain for shorter periods

Reclaiming Privacy

1. Mindful technology design
2. User empowerment/education
3. Industry practices (e.g., log retention)
4. Law
    - Statute
    - Court decisions

Principles for Legal Reform

1. Technology and platform neutrality
2. All content should be protected under the 4th A standard – regardless of how old it is or whether it has been "opened" or not
3. Data should receive same protection whether it is in transit or in storage
4. Recognize sensitivity of data that deserves 4th A protection – location data
5. Simplicity and clarity: All stakeholders – service providers, users and government investigators – deserve clear and simple rules